The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
02/02/2017

SUBJECT:
Multiple Vulnerabilities in WordPress Content Management System Could Allow for Unauthenticated Privilege Escalation

OVERVIEW:
Multiple vulnerabilities have been discovered in WordPress content management system (CMS), which could allow for unauthenticated privilege escalation. WordPress is an open source content management system for websites. Successful exploitation of these vulnerabilities could allow for unauthenticated privilege escalation allowing the attacker to compromise the affected website, or allow access to or modify data on the website.

THREAT INTELLIGENCE
There have been no reports of these exploits in the wild.

SYSTEM AFFECTED:
- WordPress versions 4.7.1 and earlier

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
WordPress issued a security and maintenance release which fixes multiple vulnerabilities in versions 4.7.1 and earlier. This security and maintenance release addresses the following vulnerabilities:
- An unauthenticated privilege escalation vulnerability was discovered in a REST API endpoint.
- The user interface for assigning taxonomy terms in “Press This” is shown to users who do not have permissions to use it.

- “WP_Query” is vulnerable to a SQL injection (SQLi) when passing unsafe data. WordPress core is not directly vulnerable to this issue, but additional hardening was added to prevent plugins and themes from accidentally causing a vulnerability.
- A cross-site scripting (XSS) vulnerability was discovered in the posts list table.

Successful exploitation of these vulnerabilities could allow for unauthorized privilege escalation allowing an attacker to compromise the affected website, or allow access to or modify data on the website.

RECOMMENDATIONS:
The following actions should be taken:

- Ensure no unauthorized systems changes have occurred before applying patches.
- Update WordPress CMS to the latest version after appropriate testing.
- Run all software as a non-privileged user to diminish effects of a successful attack.
- Review and follow WordPress hardening guidelines - http://codex.wordpress.org/Hardening_WordPress.

REFERENCES:
WordPress:
https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/
https://make.wordpress.org/core/2017/02/01/disclosure-of-additional-security-fix-in-wordpress-4-7-2/